CENTRE FOR SECURE INFORMATION TECHNOLOGIES

Muckle++ Protocol: An experimental analysis of Provably Quantum-Secure integration of QKD and PQC

Ayesha Khalid

Ciara Rafferty

Maire O' Neill

QUEEN'S UNIVERSITY BELFAST

Agenda

CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

- Motivation for a Hybrid PQC-QKD scheme
- NIST PQC Competition Update
- Muckle++ Protocol: A hybrid key exchange protocol
  - Ingredients
  - Design choices
  - Superior Security
- Implementation platform
- Performance Results
- Results
- Outlook

AQuaSeC

Agile Quantum Safe Communications (AQuaSeC)

QUANTUM COMMUNICATIONS HUB

EPSRC funded Quantum Comms Hub

Averting the Quantum threat (2 ways)

CENTRE FOR SECURE INFORMATION TECHNOLOGIES

The physical approach is QKD (Quantum Key Distribution)

- Ensures *information theoretic security*
- Security based on the laws of quantum mechanics
- Demonstrated good levels of maturity in the last decade with improved key generation rates, extending longer distances, improved scalability.

\+ Information theoretic security

− Large changes in Infrastructure and hardware, range limitations, expensive deployment

The classical approach is PQC (Post Quantum Cryptography)

- PQC refers to cryptographic schemes, thought to be secure even against quantum computers.
- Other names include *Quantum-resistant Cryptography, Quantum-Safe Cryptography*
- Major types of Post quantum cryptography include Lattice based cryptography; Code based cryptography, etc.

\+ Work on classical computers used today

− Lower maturity, standardization, research on going

Muckle[1]++ Protocol: A Hybrid Key Exchange Protocol

- A Hybrid Key exchange protocol combining the following three
  - Classical public key algorithms (**CKEM**)
  - Post Quantum KEMs (**QKEM**)
  - Quantum Key Distribution (**QKD**)

- A physical unclonable function (**PUF**) is used for device authentication
  - Providing additional layer of security

- A modular design
  - increased efficiency for different security parameters

- A working implementation with a commercial QKD, an FPGA and a server is undertaken

- This work started under **AQuaSec** (Agile Quantum Safe Communications), funded by Innovate UK.
  - Funded Period: Nov 18 - Aug 21

- A paper is submitted to **PRX Quantum** (under review)

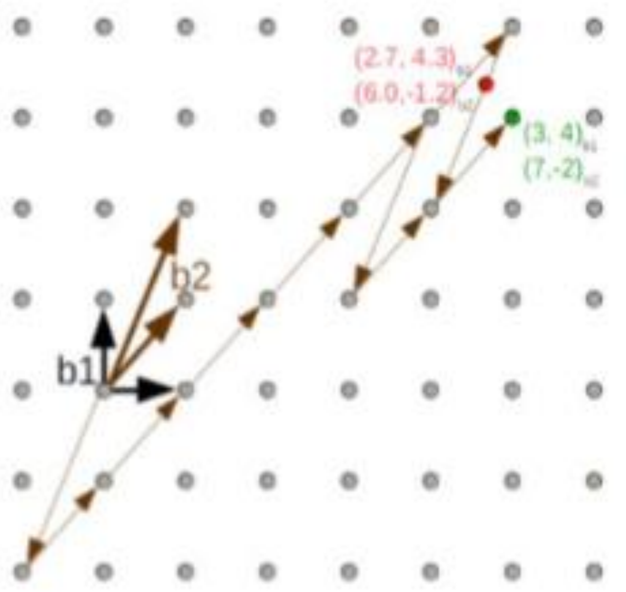
CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

[1] Dowling, Benjamin, et. Al. "Many a mickle makes a muckle: A framework for provably quantum-secure hybrid key exchange" *PQCrypto* 2020.

Muckle++: The Ingredients- Post Quantum Cryptography (Why choose lattices)

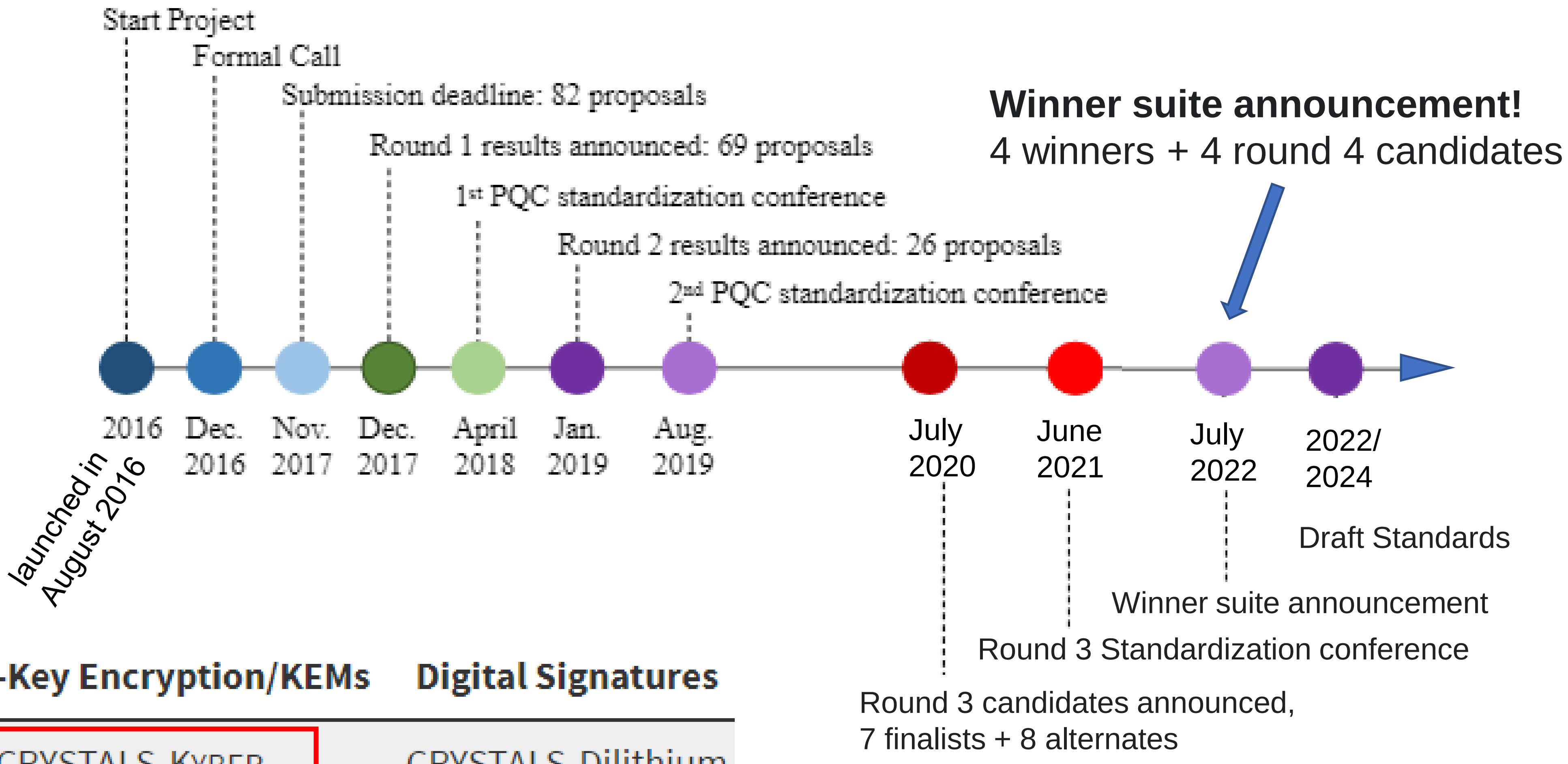
Lattice-based Cryptography is emerging as a promising PQC candidate.

- **Security**: Based on are well-studied theoretical foundations – with no known attacks
- **Flexibility**: Enable constructions beyond PKE, signatures, e.g., Identity based encryption (IBE), Attribute-based encryption (ABE), Fully homomorphic encryption (FHE).
- **Efficiency**: Simple underlying arithmetic operations, efficient on a range of diverse platforms.
  - *VPN strong Swan* supports post-quantum mode (NTRU and BLISS schemes)
  - *Google* successfully experimented with New Hope key exchange (a Lattice-based Cryptography KEM scheme)



CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

US NIST - Call for Quantum-Resistant Cryptographic Algorithms for new public-key cryptography standards (https://csrc.nist.gov/Projects/Post-Quantum-Cryptography)



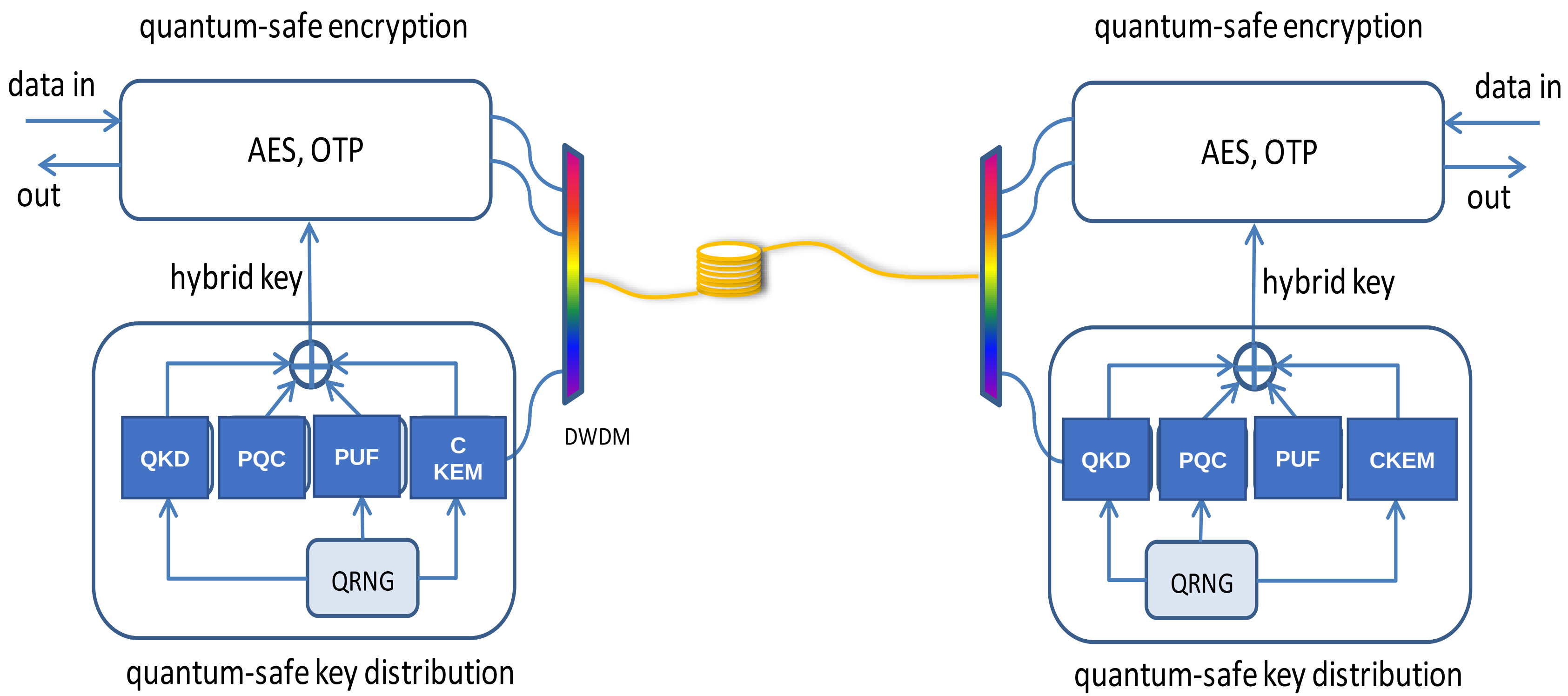
For standardization

Public-Key Encryption/KEMs	Digital Signatures
CRYSTALS-KYBER	CRYSTALS-Dilithium
	FALCON
	SPHINCS+

CENTRE FOR SECURE INFORMATION TECHNOLOGIES

Muckle++ Protocol: A hybrid key exchange protocol

- A Hybrid Key exchange protocol combining the following
  - Classical public key algorithms (**CKEM**)
  - Post Quantum KEMs (**QKEM**)
  - Quantum Key Distribution (**QKD**)
  - A physical unclonable function (**PUF**)



CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

Muckle++: The Ingredients

- Classical public key algorithms
  - **KEM**: Ephemeral Elliptic Curve Diffie- Hellman Elliptic curve (Elliptic curve curve25519)
  - ECDSA (Elliptic curve NIST P-256)

- Quantum Key Distribution (**QKD**)
  - Commercial grade QKD system[1]
  - Quantum bit error rates below 3%
  - QKD secure key rates above 3 Mb/s over a 10-dB loss channel.

- FPGA-based physical unclonable functions (**PUF**s)
  - Based on ‘Ultra-compact and robust FPGA-based PUF identification generator’ [2]

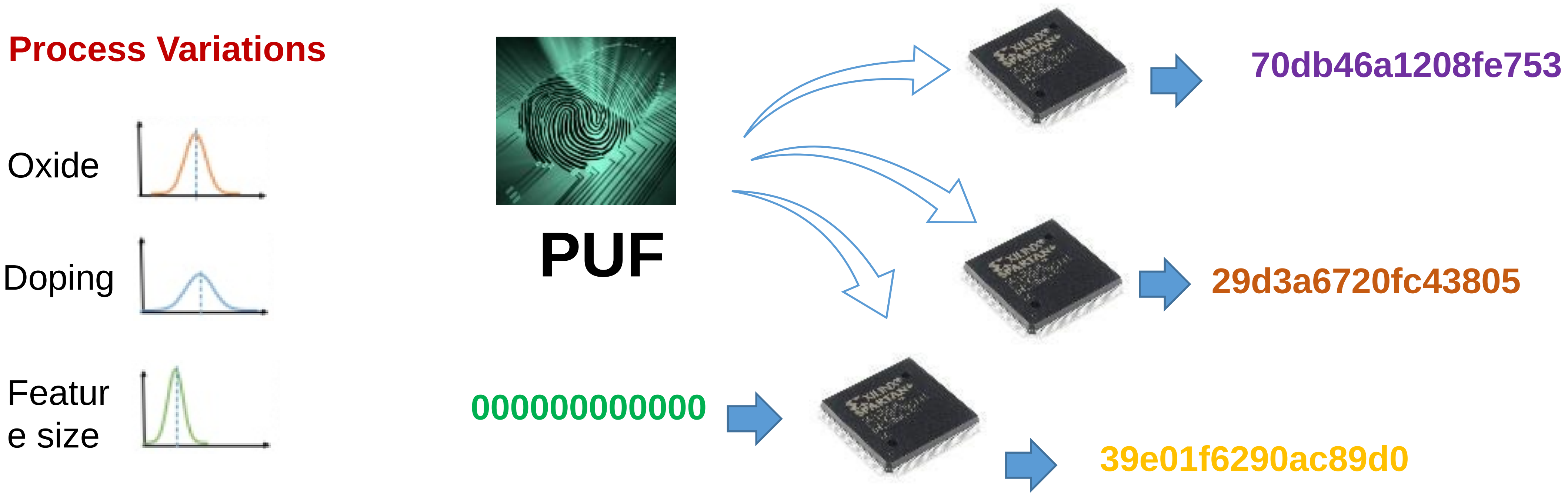
- Post Quantum Cryptography
  - **QKEM**: CRYSTALS-Kyber (n=3), mid range security
  - QSignature: Falcon (n=512, q=12289)

CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

[1] Yuan, Zhiliang, et al. "10-Mb/s quantum key distribution." *Journal of Lightwave Technology* 36.16 (2018): 3427-3433..
[2] Gu, Chongyan, and Maire O'Neill. "Ultra-compact and robust FPGA-based PUF identification generator." *2015 IEEE International Symposium on Circuits and Systems (ISCAS)*. IEEE, 2015.

Muckle++: The Ingredients- Physically Unclonable Function (PUF)

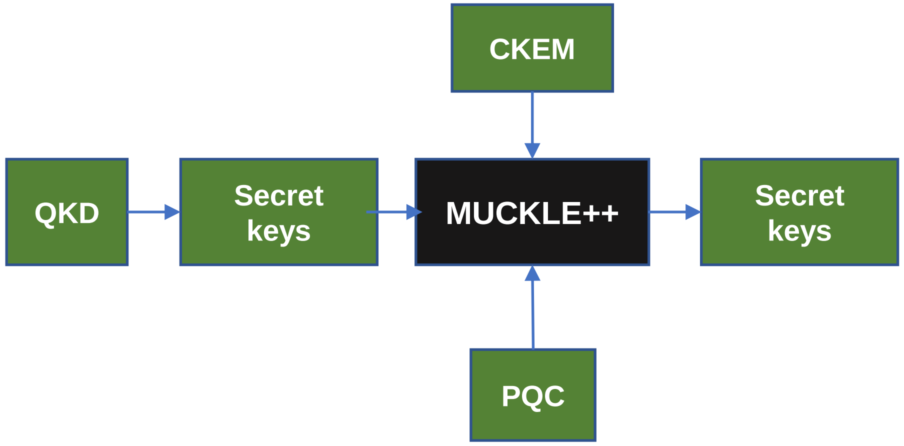
A PUF is a digital circuit that uses manufacturing process variations to generate a unique digital fingerprint.

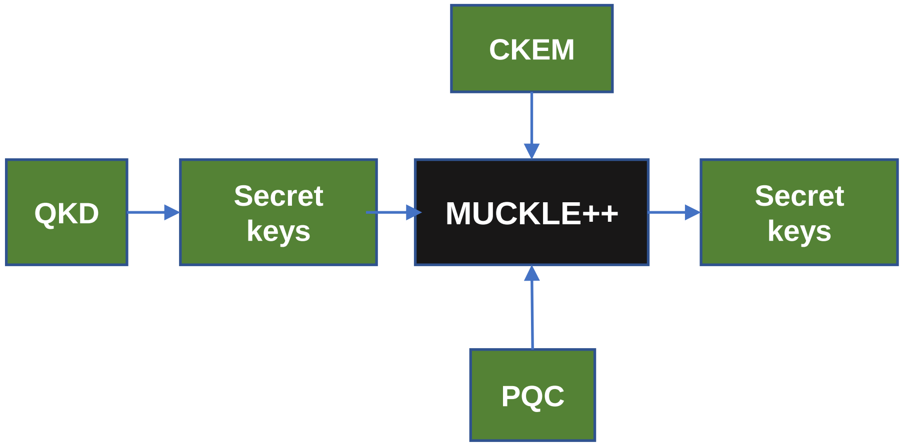


No two chips should give the same response when supplied with the same challenge.

Muckle++: Better Security Properties

- **Breakdown Resilience:** The key exchange protocol remains secure, provided at least any one of three ingredients: QKD, classical key exchange and quantum resistant key exchange, remains secure.

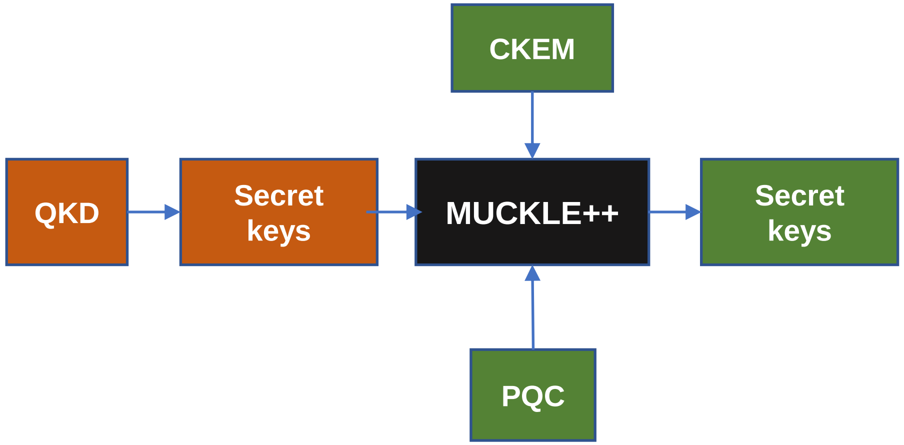


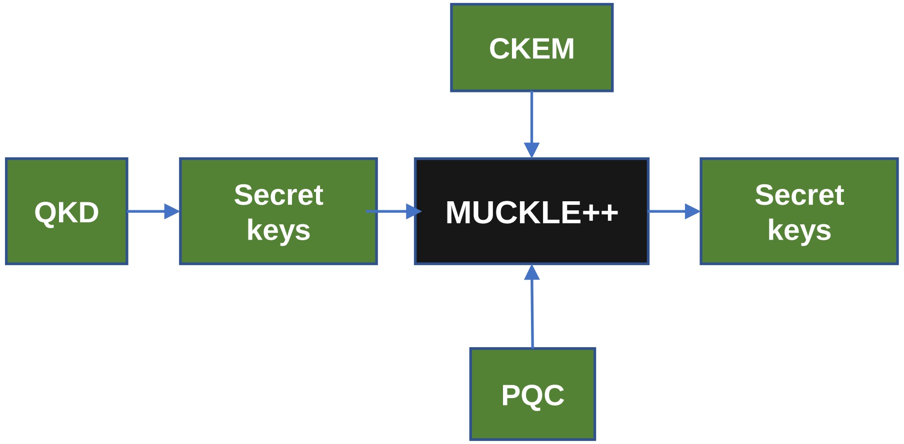


CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

Muckle++: Better Security Properties

- **Breakdown Resilience:** The key exchange protocol remains secure, provided at least any one of three ingredients: QKD, classical key exchange and quantum resistant key exchange, remains secure.



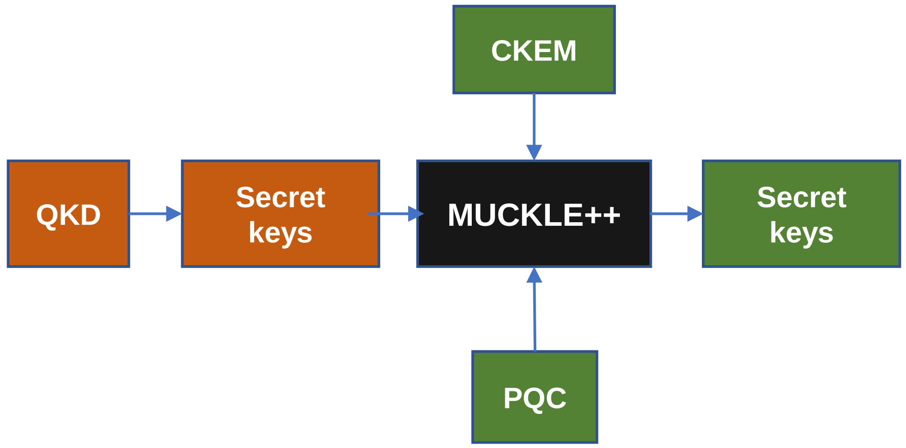


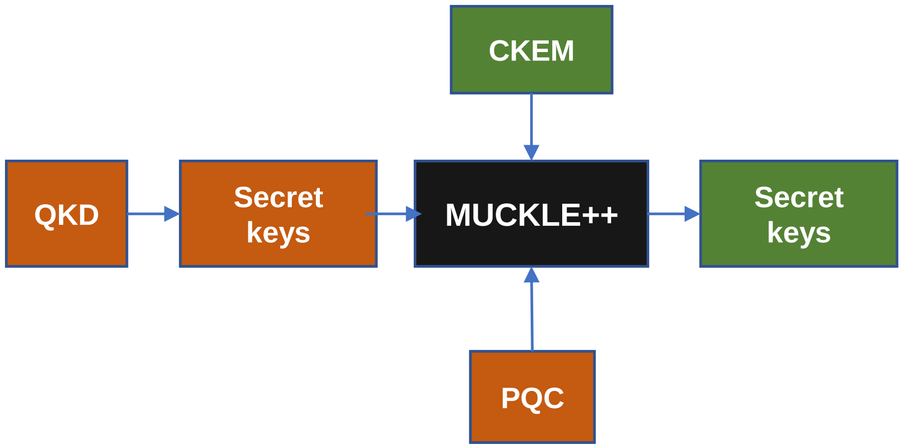
Still secure against Quantum attacks ☺

CENTRE FOR SECURE INFORMATION TECHNOLOGIES

Muckle++: Better Security Properties

- **Breakdown Resilience:** The key exchange protocol remains secure, provided at least any one of three ingredients: QKD, classical key exchange and quantum resistant key exchange, remains secure.





Still secure against Quantum attacks ☺

Only secure against classical attackers ☹

CENTRE FOR SECURE INFORMATION TECHNOLOGIES

Muckle++: Better Security Properties

- **Breakdown Resilience:** The key exchange protocol remains secure, provided at least any one of three ingredients: QKD, classical key exchange and quantum resistant key exchange, remains secure.

- **Post-compromise Security[1]:** The secret state allows for post-compromise security, that is, security can be recovered in the event of session keys being leaked.

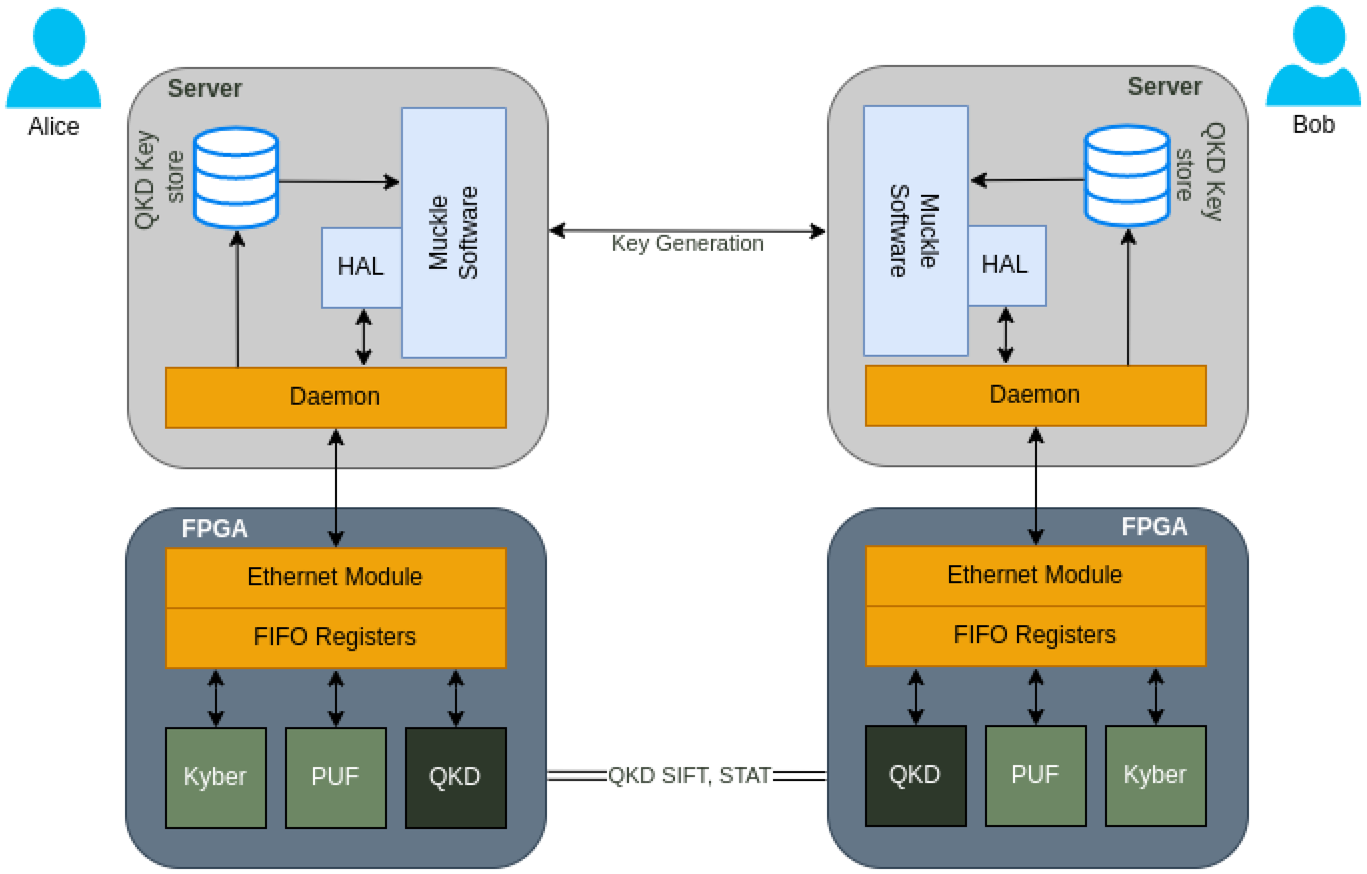
- **Forward Security**: is guaranteed, ensuring that a security breach will not affect the security of previous keys.

CENTRE FOR SECURE INFORMATION TECHNOLOGIES

[1] Cohn-Gordon, et. al.. "On post-compromise security." *2016 IEEE 29th Computer Security Foundations Symposium (CSF)*. IEEE, 2016.

Muckle++: Results

- Insecure communication channel across servers
- Muckle++ software runs on the server with a hardware abstraction layer (HAL)
- A custom Daemon enables communication with hardware IP, running on an FPGA connected via Ethernet.
- Xilinx 7-series FPGA device used



CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

Muckle++: Performance

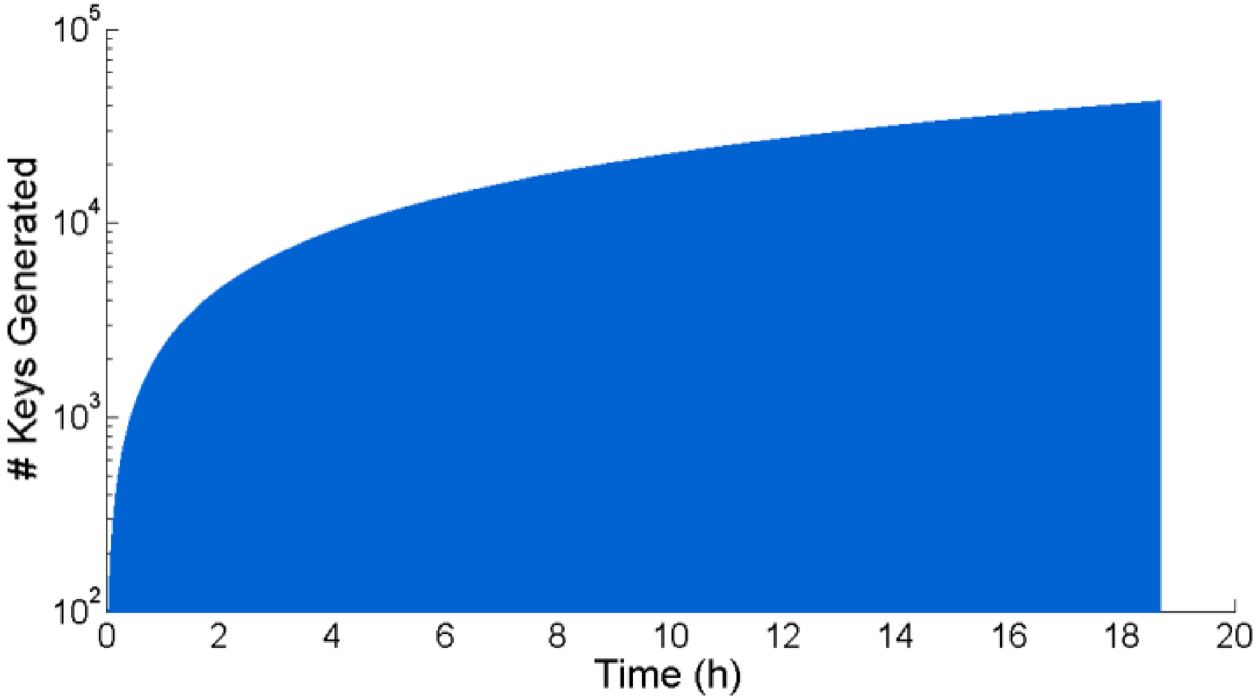
- Muckle++ protocol was run on a commercial server and connected via Ethernet to a Xilinx 7-series FPGA.

- Required time to readout the PUF response in minimal, with < 200 clock cycles required including error correction

- Running the entire system to continuously generate fresh key material led to stable operation, with one **hybrid-quantum-safe key** per second and run times > 20 hours, as shown below

Resource	Kyber	PUF
LUT	17339	4347
LUTRAM	2962	0
FF	7060	5404
BRAM	8.5	0
DSP	43	0

CRYSTALS-Kyber + PUFArea Requirements on 7-series Xilinx FPGA



	Latency (cc^a)	Latency (μs)	Operations per second
Load Secret Key	609	17.4	57471
Encapsulation	19458	555.94	1798
Decapsulation	27746	792.74	1261

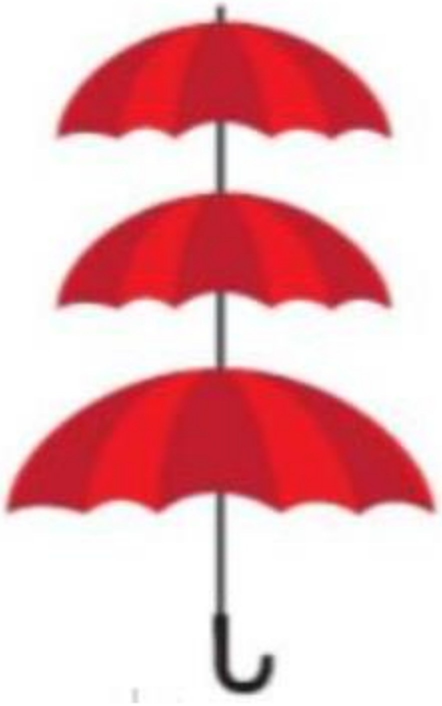
[a] clock cycles.

CRYSTALS-Kyber Performance at 35 MHz

Muckle++: Contributions

Provably Quantum-Secure integration of QKD and PQC in an authenticated key exchange protocol.

- **Post compromise security:** Security is compromised only if all the three layers of security are broken
  - Classical public key algorithms (**CKEM**)
  - Post Quantum KEMs (**QKEM**)
  - Quantum Key Distribution (**QKD**)
- **Flexibility (Modular design)**: Different building blocks can be easily swapped to allow for increased efficiency or different security parameters
- **Efficiency**:
  - Combines the best of the two worlds, integrating QKD into more practical PQC systems
  - Developed the first working implementation of the system.



CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

Muckle++: Outlook

Our work aims to pave the way for future endeavours exploiting both quantum and post-quantum technologies.

- **Efficiency:** leveraging a full hardware implementation of the Muckle++ protocol, taking advantage of FPGA-based QKD post-processing for better efficiency.
- **Investigating further use-cases:** Greater range of potential use case scenarios and applications would provide useful contributions to on-going standardisation activities
- **Vulnerability Analysis:** Undertaking vulnerability analysis of the physical security of integrated PQC-QKD designs including side channel analysis attacks and/or fault attacks.
    - *Several relevant PhD positions open currently at Queens University*. Spread the word around.

CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

Thank you

QUEEN'S UNIVERSITY BELFAST
ESTD 1845

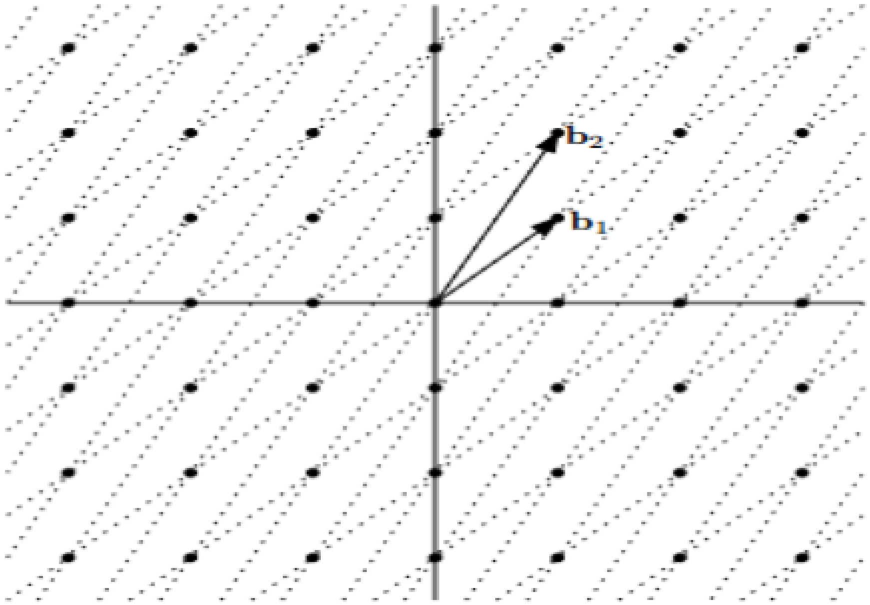
CSIT
CENTRE FOR SECURE INFORMATION TECHNOLOGIES

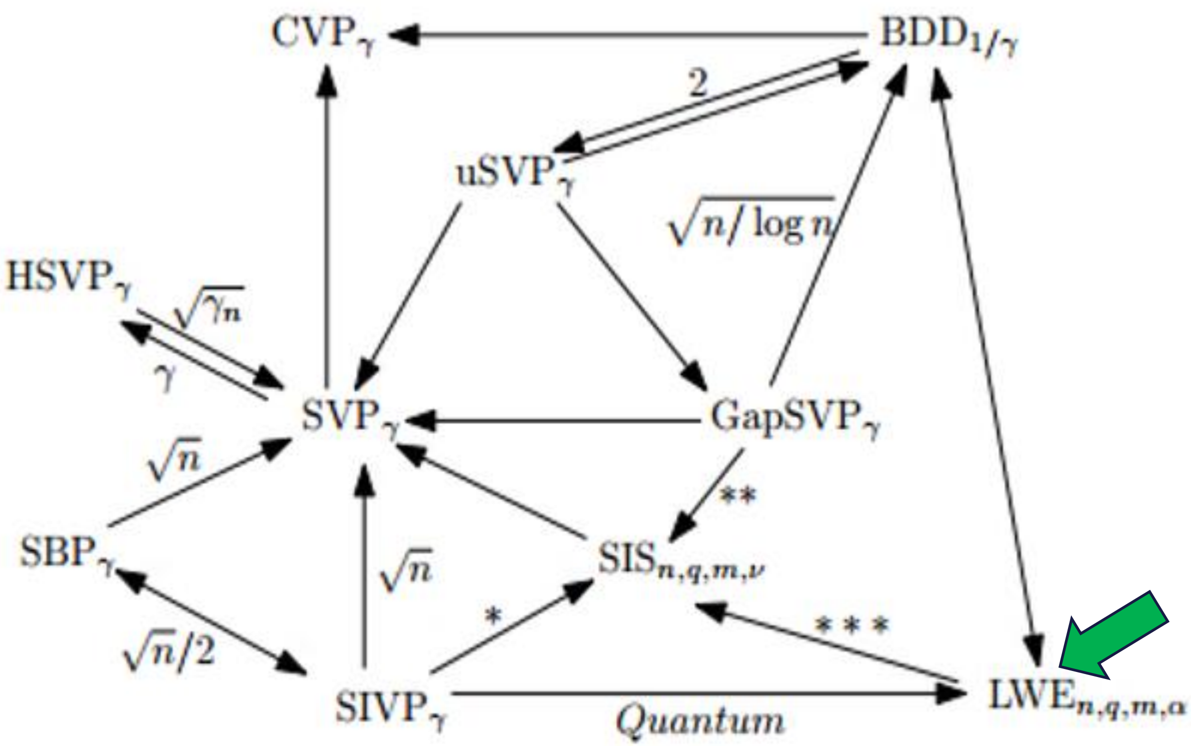
Introduction to Lattice based Cryptography

- A lattice is defined by a **basis** of **n** vectors. The lattice points can be defined by a linear combination of these basis vectors with integer coefficients

$$\boldsymbol{v} = a_1\boldsymbol{b_1} + a_2\boldsymbol{b_2} + \cdots + a_n\boldsymbol{b_n}$$

Lattice ➡ Hard problems ➡ Quantum-resilient cryptographic problems





CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

Learning with Errors problem (LWE)

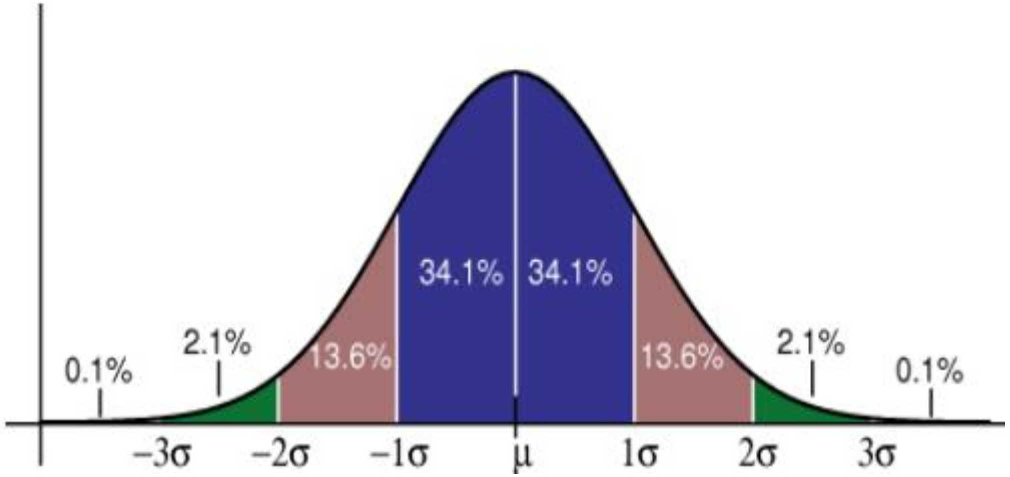
The LWE problem is defined as:

$$As + e = b \bmod q$$

Given (A, b), find s.

4 main interdependent parameters:

- Matrix A has dimension $n \times m$,
- Error vector e is chosen from a Gaussian distribution of ∂,
- All working in a field modulus q



CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

Learning with Errors problem (LWE)

Solving of a system of linear equations

secret

$$\underset{\mathbb{Z}_{13}^{7\times 4}}{\begin{bmatrix} 4 & 1 & 11 & 10 \\ 5 & 5 & 9 & 53 \\ 3 & 9 & 0 & 10 \\ 1 & 3 & 3 & 2 \\ 12 & 7 & 3 & 4 \\ 6 & 5 & 11 & 4 \\ 3 & 3 & 5 & 0 \end{bmatrix}} \times \underset{\mathbb{Z}_{13}^{4\times 1}}{\begin{bmatrix} 6 \\ 9 \\ 11 \\ 11 \end{bmatrix}} = \underset{\mathbb{Z}_{13}^{7\times 1}}{\begin{bmatrix} 4 \\ 8 \\ 1 \\ 10 \\ 4 \\ 12 \\ 9 \end{bmatrix}}$$

Use Gaussian elimination

The LWE problem is defined as:

$$\boldsymbol{As} + \boldsymbol{e} = \boldsymbol{b} \bmod q$$

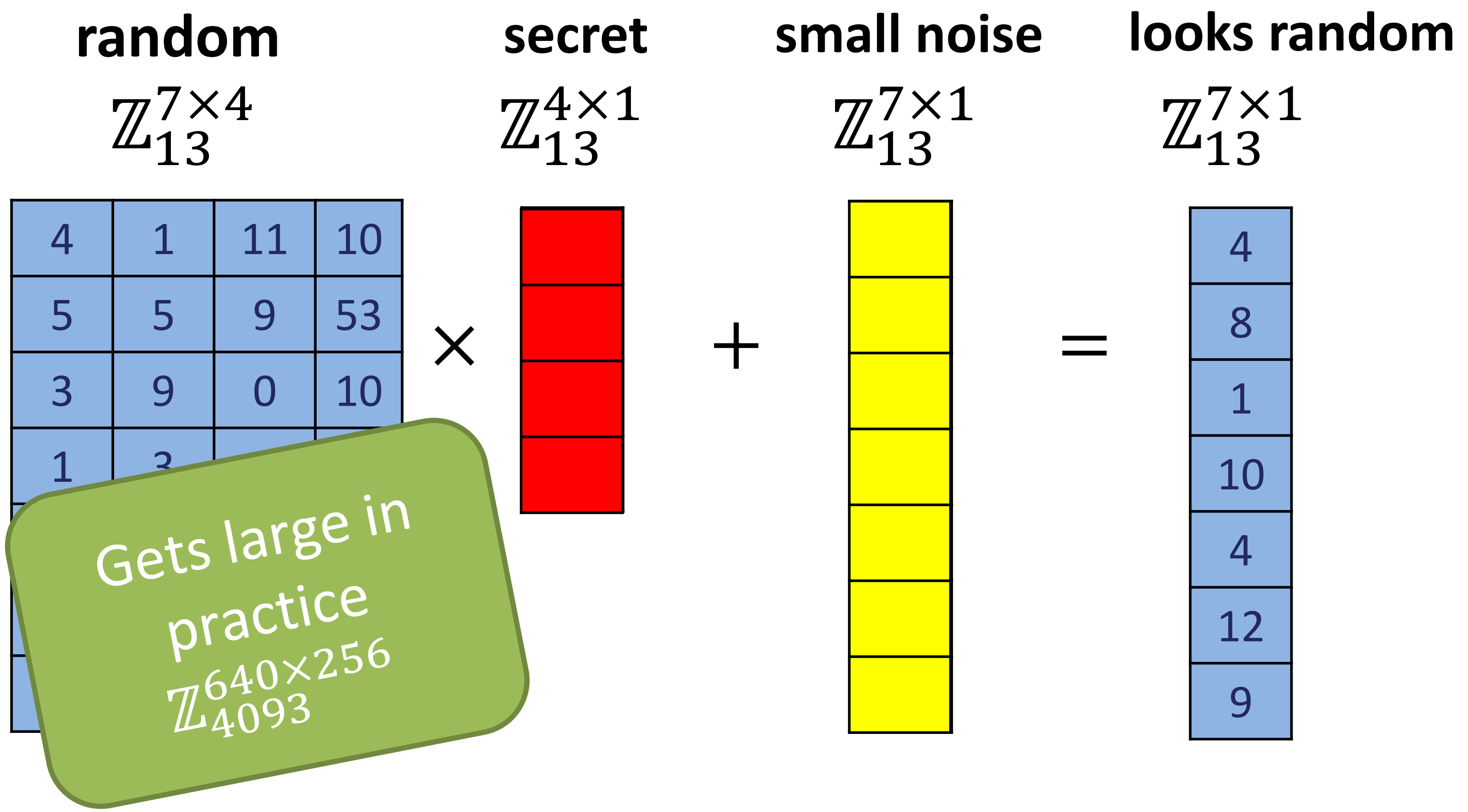
Given $(\boldsymbol{A},\boldsymbol{b})$, find $\boldsymbol{s}$.

Blue is given; Find (learn) **red** => Solve linear system

CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

(slides taken from talk by Douglas Stebila at RWC'15)

Learning with Errors problem (LWE)



Parameter sets	n	p	σ	$\lvert \boldsymbol{c}_1, \boldsymbol{c}_2 \rvert$	|sk|	|pk|	security
(256,4093,8.35 [LP11]	256	4093	~4.5	6,144	1,792	6,144	~106 bits
(256,7681,11.32) [GFSBH12]	256	7681	~4.8	6,656	1,792	6,656	~106 bits
(512,12289,12.18) [GFSBH12]	512	12289	~4.9	14,336	3,584	14,336	~256 bits

(slides taken from talk by Douglas Stebila at RWC'15)